Practical Test for System and Network Hacking

Master's Degree in Computer Engineering

3 July 2024

1. (15 points) Try out the latest release of our key-value store, featuring the patented ':' prefix for secret keys. Release notes: to further enhance security, we now support the PIE/ASLR mitigation strategy, together with some data structure reorganization that make it even more effective.

   Available commands (one per line of input):

   - `n` followed by two decimal numbers separated by a comma: create a new key-value pair; the numbers represent the size (in bytes) of the key and the value, respectively; the key and value bytes are read immediately after the command.
   - `c` remove all non-secret key-value pairs.
   - `s` followed by a string: search the pair with the given key and print its value if found (secret keys cannot be searched in this way).

   ## Hints

   1. Analysis of the bug (2 points);
   2. Attack plan (3 points).